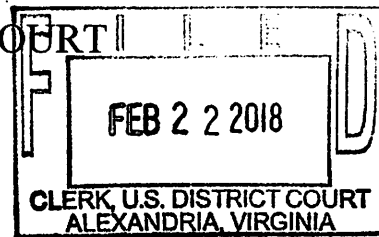


UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information Associated with an Account
at Apple, Inc., at 1 Infinite Loop Cupertino, California

Case No. 1:18sw 106

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
information associated with the account associated with the email address seanandrewduncan@gmail.com, stored at premises controlled by Apple, Inc., a company headquartered at 1 Infinite Loop, Cupertino, California.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of a crime contained in records associated with the social media accounts listed above, as further described in Attachment A. This warrant is sought also pursuant to 18 U.S.C. § 2703(c)(1)(A).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

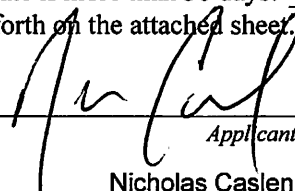
The search is related to a violation of:

Code Section
 18 U.S.C. § 2339B
 18 U.S.C. § 2252

Offense Description
 attempting to provide material support to terrorists
 possession of child pornography

The application is based on these facts:
 See Attached Affidavit


- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature
 Nicholas Caslen, Special Agent, FBI
 Printed name and title

Sworn to before me and signed in my presence.

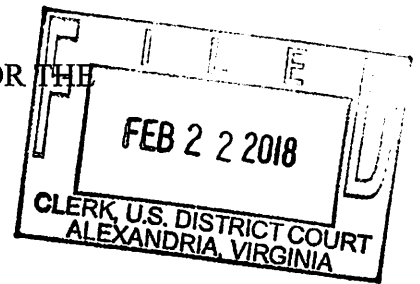
Date: 02/22/2018

City and state: Alexandria, VA

/s/ 
 Michael S. Nachmanoff
 United States Magistrate Judge
 Judge's signature
 Michael S. Nachmanoff, U.S. Magistrate Judge
 Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF)
INFORMATION TO BE PROVIDED) No. 1:18sw 106
BY APPLE, INC.)

AFFIDAVIT

I, Nicholas Caslen, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to the Washington Field Office, Joint Terrorism Task Force ("JTTF"). I have been an FBI Special Agent since 2011, and worked on the JTTF in both Wichita, Kansas, and Washington, D.C. As part of my duties, I investigate potential criminal and terrorism-related activities associated with suspected Homegrown Violent Extremists. I have participated in numerous counterterrorism investigations, during the course of which I have conducted physical surveillance, executed court authorized search warrants, and used other investigative techniques to secure relevant information regarding various crimes

2. This affidavit is submitted in support of a warrant to require the disclosure to the government of all information associated with the Apple, Inc., account associated with the email address **seanandrewduncan@gmail.com**, stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at 1 Infinite Loop, in Cupertino, California. Based on the facts contained in this affidavit, there is probable cause to believe that within the information associated with this account, are records, documents, communications, messages, and other information, more particularly described in Attachment A (and incorporated here), related to the attempt to provide material support to a designated terrorist organization, in

violation of 18 U.S.C. § 2339B, and/or the possession of child pornography, in violation of 18 U.S.C. § 2252.

3. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. I have also received information from other law enforcement and intelligence officials related to this investigation. The statements contained in this affidavit are based on my own observations, review of documents, recordings, and reliable information provided to me by other law enforcement officials. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. When in this affidavit I refer to something occurring on a specific date, I intend to convey that the event occurred on or about that date.

Probable Cause

4. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq (“AQI”), then known as Jam ‘at al Tawhid wa’al-Jihad, as a Foreign Terrorist Organization (“FTO”) under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224. On or about May 15, 2014, the Secretary of State amended the designation of AQI as a FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant (“ISIL”) as its primary name. The Secretary also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (“ISIS”—which is how the FTO will be referenced herein), the Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furquan Establishment for Media Production. On

September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

I. Duncan Possessed Evidence on Memory Chips and Thumb Drives

5. In February 2016, the FBI received information regarding Sean Andrew Duncan, (hereinafter “Duncan”), a United States citizen, who moved to Sterling, Virginia in June 2017, from Pittsburgh, Pennsylvania. One of Duncan’s relatives reported that Duncan had converted to Islam, may have been radicalized, and voiced his approval of westerners being beheaded in the Middle East. Duncan’s relative reported that Duncan and his wife planned to travel to Turkey.

6. On December 6, 2017, the FBI conducted a search of Twitter and found an account associated with the phone number 443-813-7730 (“the 7730 Phone Number”). According to an open source review of Twitter, the account was created in November 2015 and has the Twitter handle @DawlahtulIslaam. The phrase “Dawlahtul Isla[a]m” is an Arabic phrase that roughly translates to “The Islamic State.” I believe that this Twitter account was controlled by Duncan, because in November 2015, Duncan listed the 7730 Phone Number in his application for a U.S. passport.

A. Travel to Turkey

7. According to U.S. Customs and Border Protection, Duncan and his wife booked a flight to Istanbul, Turkey, departing from Washington Dulles International Airport, on February 26, 2016. The reservations reflected that Duncan and his wife were scheduled to depart Turkey for Bangladesh on March 4, 2016, and return to the United States on March 20, 2016. In fact, on February 26, 2016, Duncan and his wife departed the United States for Turkey. On February 27, 2016, they were denied entry into Turkey, and returned to the United States. Upon their return, they were interviewed by the FBI.

8. According to telephone service provider records, on March 4, 2016, Duncan changed his cell phone number from the 7730 Phone Number to a number ending in 9440 ("the 9440 Phone Number").

B. Duncan's Contact with a Foreign Detained Citizen

9. On July 25, 2017, during an interview with FBI agents, an unnamed co-conspirator (hereinafter "UCC"), who was in the custody of a foreign government for actively planning to travel to join ISIS, provided information regarding Duncan. According to UCC, Duncan was one of her U.S.-based contacts who had expressed an interest in joining ISIS, expressed an interest in conducting an attack in his homeland (the United States), and provided her instructions on how to construct homemade bombs. Duncan and UCC primarily spoke on encrypted mobile messaging applications. UCC also confirmed that she communicated with Duncan on an encrypted mobile messaging account ("MM1").

10. UCC told FBI agents she first became acquainted with Duncan on social media in January 2015 when Duncan sent her a friend request. UCC and Duncan initially communicated through social media but subsequently exchanged phone numbers and communicated on encrypted mobile messaging applications.

11. According to UCC, Duncan shared news articles with her from an ISIS news outlet known as Amaq News. During their communications in early 2015, Duncan expressed agreement with ISIS spokesman Abu Mohammad Al-Adnani's statement that Muslims should be striking their own homelands. UCC recalled that when she asked Duncan directly if he supported ISIS, he replied that he did. In addition, UCC made it clear to Duncan from the start of their relationship in the beginning of 2015 that she would not communicate with him unless he was "pro-ISIS." UCC was looking for a "Salafi or an ISIS supporter" to marry and live with in Syria.

She believed she would reap “heavenly rewards” if she married an ISIS fighter who died in battle.

12. In February 2015, UCC asked Duncan if he intended to go to Syria. Duncan told UCC that he wanted to make “hijrah” to Syria and that he wanted UCC to go with him to Syria. In order for Duncan and UCC to go to Syria together, Duncan proposed marriage to UCC. Duncan’s proposal occurred over an encrypted mobile messaging application. Duncan told UCC that after they were married, he wanted to plan their trip to Syria. Duncan wanted to come to UCC’s country to propose to UCC in person, but she said it was too soon. As a result of UCC rejecting Duncan’s offer of marriage, the two broke contact in or around March 2015.

13. UCC recalled a time before they broke contact when she was upset at work due to non-Muslim women wearing shorts that exposed their bodies. UCC told Duncan via an encrypted mobile messaging application she was upset with the way these women dressed and she wanted to do something about it. Duncan replied with a link to a website, and a message saying she could “try this.” UCC stated that the link contained pictures and instructions on how to make weapons and bombs. UCC stated the link was to an article titled, “How to build a bomb in the kitchen of your Mom” from Inspire magazine.

14. In January 2016 (a month before Duncan and his wife’s trip to Turkey), Duncan asked UCC if she still wanted to go to Syria and to be his second wife. UCC asked Duncan if his current wife would be okay with UCC coming with them to Syria. Duncan stated that his wife would have to be okay with it. UCC did not agree to go, and the two broke contact again.

15. In December 2016, Duncan, utilizing an encrypted mobile messaging account, re-initiated contact with UCC. Duncan told UCC that he had come back from Turkey, from where he and his wife had been sent back to the United States. Duncan said he thought the FBI was

monitoring him, but would not elaborate on why he was deported or why the FBI was monitoring him. Duncan said he did not want to implicate himself and that his wife could keep secrets. Duncan stated that his wife knew what to say when questioned by authorities. In July 2017, the FBI reviewed the UCC's phones and confirmed there were communications between Duncan and UCC on encrypted mobile messaging applications.

C. UCE's Interaction with Duncan

16. On August 2, 2017, the FBI identified an encrypted mobile messaging account ("MM2") with a naming convention similar to the one used by UCC to communicate with Duncan ("MM1"). A review of the profile photographs for this second encrypted mobile messaging account showed a photograph of Duncan and his father. In addition, the FBI found that MM2 was associated in the encrypted messaging application with the 9440 Phone Number.

17. On August 11, 2017, an FBI undercover employee (UCE) posing as UCC, contacted Duncan, who was using MM2. UCE told Duncan that "she" had been arrested by foreign authorities. Immediately after being told this, Duncan created secure chats and self-destruct timers to destroy the content of his messages with UCE. UCE told Duncan that "she" intended to make "hijrah." Duncan stated, "Hm, you know a fence Someone to take you, and is it safe in Iraq." Later, UCE asked Duncan if he had a contact in Syria, to which Duncan responded, "No a couple have been marytred (sic)."

18. On August 20, 2017, UCE told Duncan that "she" was in contact with an individual in Libya who was attempting to facilitate "her" travel to Libya. UCE told Duncan that the Libyan contact was asking various vetting questions prior to assisting UCE. UCE told Duncan that "her" Libyan contact was asking strange questions, such as UCE's blood type and family contact. UCE then asked Duncan if he (Duncan) and his wife were asked similar questions when

they tried to travel to Syria. Duncan stated, “they won’t ask that.” Duncan further stated, “I didnt (sic) go for that Just honeymoon.”

19. However, later in the conversation, UCE asked Duncan what to do about “her” contact in Libya. Duncan recommended that UCE “. . . lie to him.” Duncan stated he had never dealt with unnecessary vetting by “contacts” and that he had “always had referrals.” Based on my training and experience, I know that ISIS uses a referral system to recruit new members, and I interpret Duncan’s statement to mean that Duncan did not get asked questions by his contacts because he had “referrals” who could give them “tazkiyah.” Tazkiyah is a recommendation from a Jihadi Shaykh from their homeland or a Mujahid already in the land of Jihad. It is a generally given by an existing member of ISIS to show an individual is trustworthy.

D. Evidence from a Detained ISIS Supporter

20. In October 2017, a foreign government (not the one in whose custody UCC was) arrested one of its nationals (“Recruiter 1”) for inciting rebellion. Recruiter 1 is an ISIS recruiter who is suspected of drawing foreign fighters from around the world to Recruiter 1’s home country using social media. Recruiter 1 was married to two jihadis with connections to ISIS, one of whom is dead and the other of whom was arrested for extremism by his home country. Recruiter 1 posted a message on an electronic messaging application soliciting local and foreign Muslims to help terrorists fight government troops in Recruiter 1’s home country.

21. On December 4, 2017, during an interview with FBI agents, Recruiter 1 said she had begun recording the names and telephone numbers of individuals who had requested to join her Telegram, Facebook, or other social media and/or communication application groups. Recruiter 1’s notes included a handwritten name appearing to be “Sean Ibn Gary Duncan,” associated with the 7730 Phone Number and the associated username MM1.

E. Duncan's Phone History Research to Conduct Attacks

22. On June 29, 2017, the Allegheny County Police Department ("ACPD") provided a partial copy of Duncan's phone to the FBI. On October 6, 2017, ACPD provided the remainder of the copy to the FBI. ACPD had obtained this copy during an investigation surrounding the recent death of Duncan's infant child (the cause of death in the autopsy was inconclusive).

Duncan consented in writing to ACPD's search of his phone. The FBI's review of Duncan's imaged phone revealed hundreds of internet searches between March 2017, and June 2017, for ISIS-related materials; weapons; terrorists; body armor; surveillance; defense tactics; watchlist statuses leaked, watchlist terms, watchlist explanations. Based on my training and experience, I know the above-described searches are consistent with research into how to conduct an attack and defend oneself.

II. The Search of Duncan's Residence and Obstruction of Justice

23. On December 19, 2017, United States Magistrate Judge Theresa Carroll Buchanan authorized searches of Duncan's 2013 Honda CRV automobile, as well as his residence on Courtyard Square, in Sterling, Virginia, for evidence of attempts to provide material support to ISIS, in violation of 18 U.S.C. § 2339B, as well as false statements, in violation of 18 U.S.C. § 1001. Among the items authorized for seizure in the search were files or information (including files or information on computers or phones) involving travel or attempts to travel overseas; communications with members of foreign terrorist groups, and/or foreign or U.S.-based radicalizers or facilitators, or co-conspirators; contact lists of individuals associated with foreign terrorist groups, and/or foreign or U.S.-based radicalizers or facilitators; records of internet activity, or other information identifying support for or research related to a foreign terrorist

group; and information, programs, tools or applications that may be used for overt or clandestine/covert communications, and any associated contacts or communications history.

24. On December 29, 2017, FBI agents executed the search warrants at Duncan's residence and automobile. Upon execution of the warrant at the residence, the agents knocked on the door, identified themselves as FBI, and announced that they were there to execute a search warrant. Receiving no response, the agents knocked and announced their presence again, but received no response again. The agents then forcibly opened the door, and again identified themselves as FBI, and that they were there to execute a search warrant. The agents at the front door did not see anyone.

25. Moments before the FBI agents entered the residence through the front door, Duncan ran out the back door, barefoot, and with something clenched in his fist. FBI agents guarding the back door yelled at Duncan to stop. Before stopping, Duncan threw a plastic baggie over the heads of the agents.

26. FBI agents recovered the baggie thrown by Duncan. The baggie was a clear plastic Ziploc bag, containing a memory chip stored within a thumb drive that had been snapped into pieces, and placed in a liquid substance that produced frothy white bubbles. Upon searching Duncan, agents recovered a broken casing for a thumb drive from Duncan's pants pocket.

27. Based on my training and experience, I know that thumb drives can be plugged into computers and used to store large gigabyte amounts of electronic information, to include images and documents. Based on my training and experience, I know that criminals, including terrorists and individuals involved in other crimes such as child pornography, often use thumb drives to store evidence of their criminal activity that they do not want found on their computers.

28. In light of the circumstances, I believe that Duncan fled from the house with the baggie and the memory chip and the broken thumb drive in order to conceal those items from the FBI agents that Duncan knew were about to search his house. Further, I believe that the thumb drive was snapped in pieces because Duncan altered, destroyed, and mutilated it in order to impede and obstruct the FBI's investigation of him. Similarly, based on the circumstances, I believe that the memory chip and broken thumb drive was contained in a baggie containing a liquid substance because Duncan altered, destroyed, and mutilated it in order to impede and obstruct the FBI's investigation of him.

III. Child Pornography

29. On December 29, 2017, and again on January 1, 2018, while reviewing one of the electronic devices obtained as a result of the search warrant referenced in the complaint for evidence pertaining to violations of Title 18, United States Code, Sections 1001 and 2339B, an FBI Agent observed images of what appeared to be child pornography contained within the device. Based on my training, experience, and the facts set forth below, the FBI believes that the images constitute violations of Title 18, United States Code, Sections 2252 and 2252A.

30. One item seized was a Samsung Galaxy Note 3 smartphone ("the Samsung"). On December 29, 2017, and again on January 1, 2018, while reviewing the Samsung, an FBI Agent observed images of pre-pubescent minors that appeared to be engaged in sexually explicit conduct with adult males. The images appeared to be child pornography. An FBI Agent observed other images of pre-pubescent minors posed to expose their genitalia in a sexual manner, which also appeared to be child pornography. Several of the images appeared to be screen shots of viewed websites. The pre-pubescent minors in the photos were as young as infants, and the total number of images was in the hundreds.

31. The Samsung smartphone containing the images of suspected child pornography was, in the past, registered to the 7730 Phone Number that belonged to Duncan.

32. On January 4, 2018, United States Magistrate Judge Theresa Carroll Buchanan authorized searches of electronic devices and materials seized from Duncan's residence and automobile on December 29, 2017, for evidence of the possession of child pornography, in violation of 18 U.S.C. § 2252 and 2252A.

33. After further review of two of the electronic devices obtained as a result of the search warrant referenced in the complaint for evidence pertaining to violations of Title 18, United States Code, Sections 1001 and 2339B, an FBI agent observed images of what appeared to be bloodied, deceased children located in a conflict zone similar to Syria or Iraq. There were also hundreds of images of beheadings of adult men, ISIS fighters and propaganda videos promoting ISIS extremism.

IV. Electronic Communication Accounts Identified

34. In addition to seizing the Samsung smartphone mentioned above, the FBI also seized an iPhone from Duncan's residence on December 29, 2017.

35. A review of the iPhone revealed that it contained a MSISDN number ending in 9440, which matched Duncan's previous known phone number ending in 9440. Further review of the iPhone revealed an SMS message on January 10, 2017, between the user and other individual, during which the user of the iPhone identified themselves stating, "...this is Sean."

36. As mentioned earlier, during the course of the investigation into Duncan, the FBI learned Duncan used social media platforms and mobile messaging applications to communicate with ISIS sympathizers overseas. Duncan was in contact with at least two individuals supportive

of ISIS, both whom have been arrested by national security law enforcement agencies in their home countries.

37. Based on Duncan's use of social media and mobile messaging applications to communicate with at least two known ISIS related individuals, I believe Duncan utilized his social media, emails, and mobile messaging to engage with other ISIS members and/or prospective members. I believe that Duncan may have used those electronic accounts to express his desire to join ISIS, to communicate with ISIS recruiters, and to send bomb-making information to others.

38. In addition, because child pornography was already found on electronic media belonging to Duncan, and because perpetrators of crimes involving child pornography often possess child pornography on multiple electronic devices, I submit there is probable cause to believe that Duncan collected digital images of child pornography using various electronic accounts, and stored those images on various cloud storage accounts such as those described below.

39. Furthermore, based on my training, experience, and discussions with other agents, I know that individuals involved in criminal activity such as terrorism and possession of child pornography, utilize email providers such as Google and Yahoo, as well as social media platforms to include Facebook, Instagram, Twitter, and Snapchat to communicate with other individuals involved in similar criminal activity. I also know that social media platforms such as Tumblr have features that allow users to connect with other users, chat with other users, and share content on a user's page, which can be used to further criminal activity related to terrorism

and possession of child pornography. In addition, I know based on my training and experience that email providers such as Yahoo! offer services to individuals who use their products such as cloud storage for computer files, calendars, chat features, and even social media pages. I know that individuals involved in criminal activity, such as terrorism and possession of child pornography, tend to store files such as photographs in the cloud storage provided to them by companies such as Yahoo! I further know that internet websites such as, Apple accounts, Dropbox and Evernote provide users similar types of cloud storage. Therefore, based on my training, experience, and discussions with other agents, I know that individuals who Dropbox and Evernote could use the features provided to further criminal activity related to terrorism and possession of child pornography. For these reasons, and those detailed above, I submit that there is probable cause to believe that evidence of Duncan's attempt to support terrorism and possession of child pornography will be located in the following electronic facilities, belonging to Duncan.

40. During the FBI's reviews of the iPhone, it was discovered that the Apple ID associated with the phone is associated with email **seanandrewduncan@gmail.com**. On January 19, 2018, I attempted to create an Apple ID account using the email address **seanandrewduncan@gmail.com**. The attempt failed, and I was provided the following information by Apple: "This email address is not available. Choose a different address." Therefore, I believe that Duncan's Apple ID account associated with the email **seanandrewduncan@gmail.com** is still active.

41. Based on my training and experience, I know the following about Apple, Inc.:

- a. Apple, Inc., a company headquartered at 1 Infinite Loop, in Cupertino, California, produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage.
- b. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- c. Message and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“Messages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- d. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- e. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices, i Works Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
- f. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.
- g. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and delete (or “wipe”) the contents of those devices.

- h. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth to determine a user’s approximate location.
- i. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content - including music, movies, and television shows - can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.
- j. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.
- k. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the IP address used to register and access the account, and other log files that reflect usage of the account.
- l. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot

pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

- m. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.
- n. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.
- o. Apple iCloud is used to store backups of iPhone, iPad, and iPod devices in the cloud. Apple iCloud storage can be used for iCloud backup, iCloud drive, iCloud photo library, iCloud mail (using the @icloud.com account), and data from Apps that use iCloud. Apple can create iCloud backups of an iPhone's content directly from the iPhone when connected to a Wi-Fi network. In such instance, the iPhone can be

configured under “Settings” to perform a backup of the phone over the Internet. Accessing the iCloud account provides the ability to manage devices online, including locating the iPhone or deleting (“or wiping”) its contents. Data from an iPhone can also be erased manually from the iPhone. Files deleted within the last 30 days can be recovered from the iCloud drive.

42. Therefore, the computers of Apple, Inc. are likely to contain all the material described above, including stored electronic communications and information, such as account access information, transaction information, and other account information.

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Apple, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Section A of Attachment A, government-authorized persons will review that information to locate the items described in Section B of Attachment A.

44. I am trained and experienced in identifying communications relevant to the crimes under investigation, but personnel of Apple, Inc. are not. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence, but employees of Apple, Inc. are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer networks of Apple, Inc. for the relevant account and then to analyze the contents of that account on the premises of that corporation. Further, the impact on the business of that corporation would be severe.

45. Accordingly, executing a warrant to search an account at Apple, Inc. requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject accounts in this case for evidence of the target crimes will require that agents cursorily inspect all information produced by Apple, Inc. in order to ascertain which contain evidence of that crime, just as it necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to identify all of the information subject to seizure, because keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

46. In order to facilitate seizure by law enforcement of the records and information sought from Apple, Inc. through this affidavit and application with a minimum of interference with the business activities of Apple, Inc. and to protect the rights of the subject of the investigation, and to effectively pursue this investigation, this application seeks the issuance of a warrant that would permit employees of Apple, Inc. to assist agents in the execution of this warrant, in accordance with the procedures described in Attachment A to the warrant, which is hereby incorporated into this affidavit.

47. I am advised that, pursuant to 18 U.S.C. § 2703(a), a Court with jurisdiction over the offense that is under investigation has authority to issue a warrant to compel disclosure of stored content and records and other information pertaining to a customer or subscriber of an electronic communication service including a provider located physically in another judicial


district. Accordingly, this Court has the authority to issue warrants to Apple, Inc. for stored content and records and other information pertaining to its subscribers even though that business is located in California.

Conclusion

48. Based on the information set forth above, I submit there is probable cause to believe that the information associated with the email account **seanandrewduncan@gmail.com**, stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at 1 Infinite Loop, in Cupertino, California, contains evidence of an attempt to provide material support to a designated terrorist organization, in violation of 18 U.S.C. § 2339B, and/or the possession of child pornography, violation of 18 U.S.C. § 2252, as more particularly described in Attachment A.

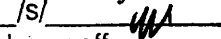
Wherefore, I request the issuance of a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

FURTHER THIS AFFIANT SAYS NOT.



Nicholas Gaslen
Special Agent, FBI

Subscribed to and sworn before me on this 22nd day of February 2018.



Michael S. Nachmanoff
United States Magistrate Judge

Michael S. Nachmanoff
United States Magistrate Judge

ATTACHMENT A (Apple, Inc.)

A. The search warrant will be presented to Apple, Inc. personnel who will be directed to isolate information in the Apple, Inc., account associated with the email address **seanandrewduncan@gmail.com**. Apple, Inc. employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the account specified above, including an exact duplicate of all information stored in the computer accounts and files described therein, including:

- a. The content of any and all cloud storage and other accounts;
- b. All records or other information regarding the identification of the accounts described in Attachment A above, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of services utilized, the IP address used to register the account, log-in IP address associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number) provided by the subscriber to Apple, Inc.;
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, to include any and all contacts listed on the subscriber's contact list, pictures, and files, to include any and all contents of electronic files that the subscriber has stored; and
- d. All records pertaining to communications between Apple, Inc. and any person regarding the account, including contacts with support services and records of action taken.

B. Law enforcement personnel will thereafter review all information and records received from the Apple, Inc. employees to determine the information to be seized by law enforcement personnel. The information to be seized consists of information related to the attempt to provide material support to a designated terrorist organization, in violation of 18 U.S.C. § 2339B, and/or the possession of child pornography, in violation of 18 U.S.C. § 2252, including records relating to the identities of those who created, used, or communicated with the account.